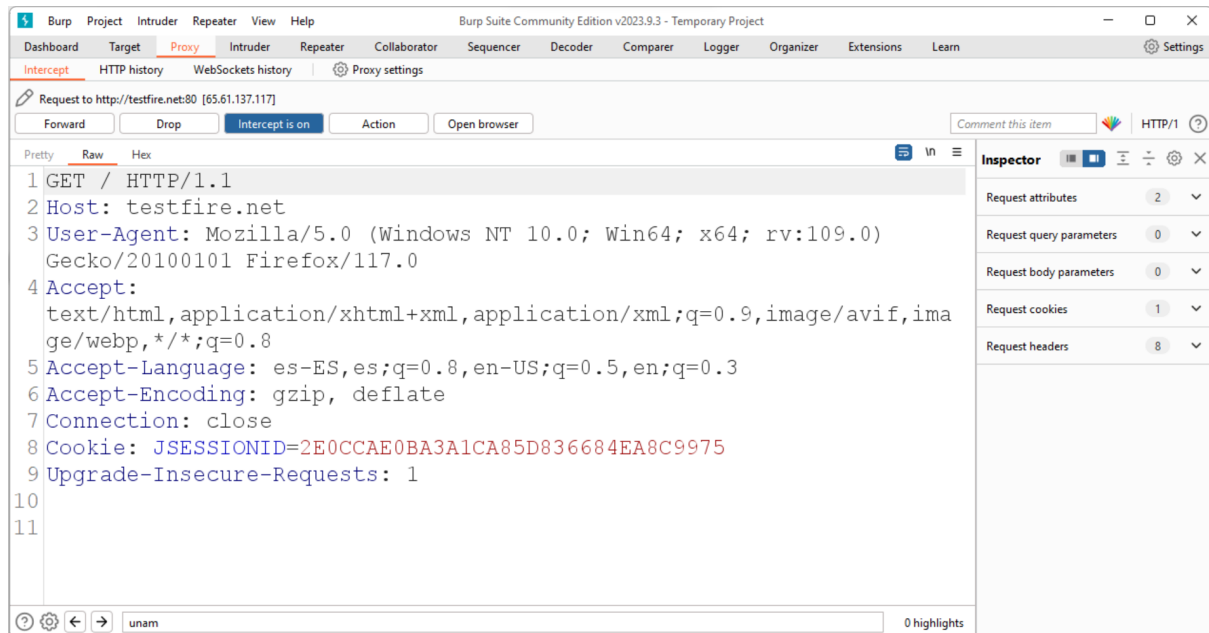


Uso de Burp Suite y análisis de la cabeceras regresadas



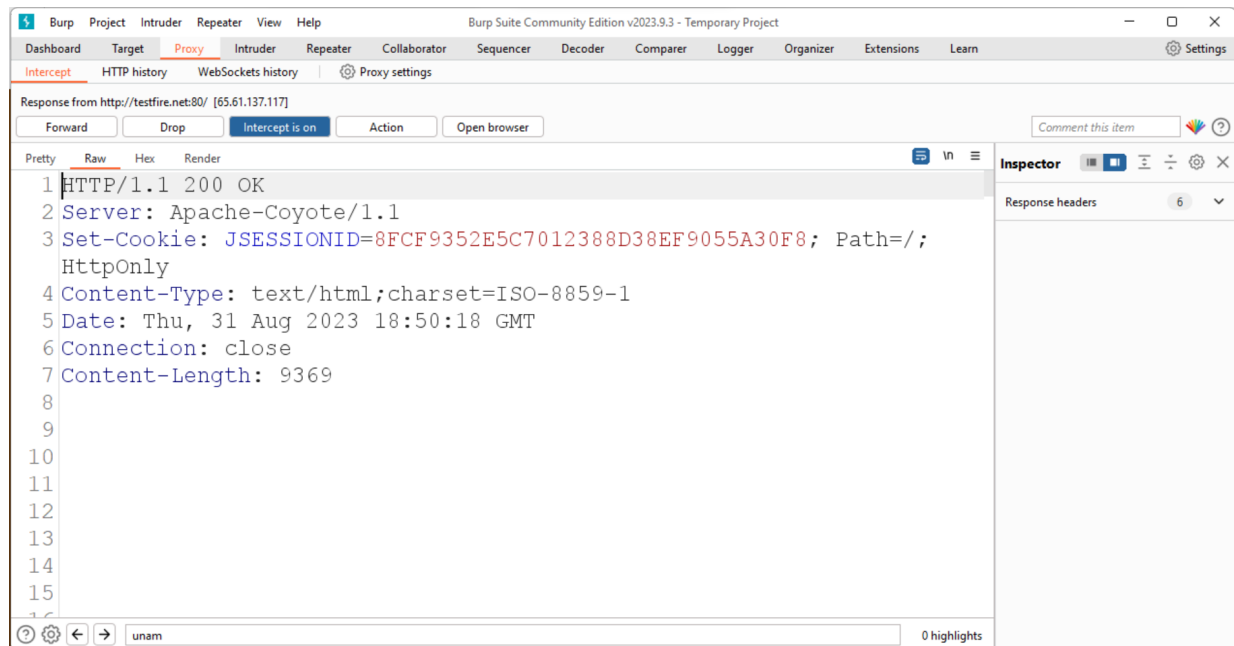
Cabeceras y/o Request

las tres cabeceras más importantes son host, user-agent, content-type

- Get: es un método que nos va a permitir solicitar de (cliente) a (servidor) los métodos http nos permite hacer solicitudes de recursos
- /: después de esta diagonal ingresamos el recurso a solicitar
Recurso solicitado HTTP /1.1 ó /1.0 Versión del recurso
- User-Agent: contiene sistema operativo, versión, descripción del software según el user-Agent la página se modifica y se comporta diferente su visualización con esto evitamos algún tipo de identificador
- Accept: tiene el formato que contendrá la página
- Accept-Language: contiene los lenguajes
- Accept-Encoding: tipos de cifrados que acepta
- Referer: es la aplicación web anterior, crf, evade mecanismos de autenticación; Escalar entre recursos
- Connection : close
- cookie: nos identifica como clientes y se mantendrá después de cerrar cada petición el servidor nos da un id al hacer la conexión, al identificarnos como en un login nos da un id de cookie

broken authentication = cuando no tengo id en el cookie

La respuesta 200 nos dice que la petición se hizo y concluye correctamente



Server: el tipo de servidor que se está corriendo y su versión, es una vulnerabilidad

Set-Cookie: es nuestra sesión asignada, el servidor nos está dando esta cookie el servidor para identificarnos

Content-Type: nos dice que nos está regresando puede regresar código html de tipo texto, puede regresar código, imágenes u otros tipos

Date: nos dice la fecha de la request

Connetion:

Content-Length: cuantos caracteres contiene

La response jamas se modifica, solo modificaremos código html,

códigos de estado:

200*: se completo correctamente

203

204*: se completo la petición pero no hay nada de vuelta

206

301*: caído definitivamente

302*: temporalmente

303:

304*: nos regresa las cabeceras con tipo caché puesto que no se ha modificado nada y se está trabajando dentro del mismos cache

401: sintaxis inválida

404:

418tipop

500

501

504

505

503

errores de cliente

errores de servidor

